Contextual anomaly detection for cyber-physical security in Smart Grids based on an artificial neural network model - DTU Orbit (09/11/2017)

Contextual anomaly detection for cyber-physical security in Smart Grids based on an artificial neural network model

This paper presents a contextual anomaly detection method and its use in the discovery of malicious voltage control actions in the low voltage distribution grid. The model-based anomaly detection uses an artificial neural network model to identify a distributed energy resource's behaviour under control. An intrusion detection system observes distributed energy resource's behaviour, control actions and the power system impact, and is tested together with an ongoing voltage control attack in a co-simulation set-up. The simulation results obtained with a real photovoltaic rooftop power plant data show that the contextual anomaly detection performs on average 55% better in the control detection and over 56% better in the malicious control detection over the point anomaly detection.

General information

State: Published
Organisations: Department of Electrical Engineering, Center for Electric Power and Energy, Energy system operation and management
Authors: Kosek, A. M. (Intern)
Number of pages: 6
Publication date: 2016

Host publication information

Title of host publication: 2016 Joint Workshop on Cyber-Physical Security and Resilience in Smart Grids
Publisher: IEEE
ISBN (Print): 978-1-5090-1164-3
Main Research Area: Technical/natural sciences
Workshop: 2016 Joint Workshop on Cyber-Physical Security and Resilience in Smart Grids, Vienna, Austria, 12/04/2016 - 12/04/2016
Anomaly detection, Intrusion Detection Systems, Smart grid, Data analysis, Cyber-physical security
DOIs:
10.1109/CPSRSG.2016.7684103

Relations

Activities:
2016 Joint Workshop on Cyber-Physical Security and Resilience in Smart Grids
Source: PublicationPreSubmission
Source-ID: 123575742
Publication: Research - peer-review › Article in proceedings – Annual report year: 2016